THE FACTS: ONLINE SHOPPING

Online shopping is convenient, easy, and quick. But it's wise to make sure you're protected before you start adding items to your cart.

What can I do to protect myself when shopping online?

-- Make sure your security software, web browsers and operating system are up to date. Keeping a clean machine is the best defense against viruses, malware, and other online threats.
-- Check out sellers: Conduct independent research before you buy from a seller you have never done business with. Some malicious websites appear to be legitimate, so you should verify the site before supplying any information. Search for merchant reviews.
-- Locate and note phone numbers and physical addresses of vendors in case there is a problem with your transaction or your bill.
-- Make sure the site is legitimate: Before you enter personal and financial information, look for signs that the site is secure. These include a closed padlock on your web browser's address bar or an address that begins with shttp or https. This indicates that the purchase is encrypted or secured. Never use an unsecured wireless network to make an online purchase.
-- Protect your personal information: When making a purchase online, be alert to the kinds of information being collected to complete the transaction. Make sure you think it is necessary for the vendor to request that information. Remember, you only need to fill out required fields on a vendor's checkout form.
-- Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your information will be stored and used.
-- Use safe payment options: Credit cards are generally the safest option because they allow buyers to seek a credit from the issuer if the product isn't delivered or isn't what was ordered. Also, unlike debit cards, credit cards may have a limit on the monetary amount you will be

responsible for paying if your information is stolen and used by someone else.
-- Never send cash through the mail or use a money-wiring service, because you'll have no recourse if something goes wrong.
-- Don't forget to review return policies. You want a no-hassle ability to return items.

-- Keep a paper trail: Print and save records of your online transactions, including product description, price, online receipt, terms of sale, and copies of any email exchanges with the seller.
-- Read credit card statements as soon as you get them to make sure there aren't any unauthorized charges. If there is a discrepancy, call your bank and report it immediately.
-- Turn your computer off when you're finished shopping: Leaving your computer running and connected to the Internet day and night gives scammers 24/7 access to install malware and commit cyber crimes.
-- Be wary of emails requesting information: Attackers may attempt to gather information by sending emails requesting that you confirm purchase or account information. Legitimate businesses will not solicit this type of information through email. Contact the merchant directly if you are alerted to a problem using contact information found on your account statement, not in the email.

SOURCE: National Cyber Security Alliance Cyber Threat Resources booklet, November 2012

Follow ARCYBER on
(click the images to visit our pages)

ABOUT US: United States Army Cyber Command directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.

As of 2 March 2016